Introduction

Mobile operators are migrating to the All IP networks. Companies such as Verizon Wireless and AT&T Wireless have national footprint and have VoIP gateways at different geographical locations (e.g., east coast and west coast). The mobiles can roam in the US to a location far away from their home system. It would be nice to be able to route incoming VoIP calls to the mobiles as close as possible to where the roaming mobiles are.

Problem Statement

When mobile operators have IP-interconnections with other operators, mobile or non-mobile, the routing of an incoming VoIP call to their telephone number (TN) would be to a specific IP gateway of the destination mobile operator that covers the geographical area of the destination TN.

When a mobile roams from an east coast system to a west coast system, an incoming VoIP call from mid-west or west coast area to such a roamer would be terminated to the IP gateway in the east coast and then routed to a west coast system. So the call routing in the IP domain is not optimal for destination mobiles that are roaming.

Previous Options

When handling a VoIP call, the originating or transit network may be configured to route the call to one of the destination mobile operator's IP gateways based on the destination TN's geographical area or use the VOICE Uniform Resource Identifier (URI) information that is provisioned in the NPAC for the destination TN by the mobile operator who serves that TN.

The VOICE URI information that is provisioned by a mobile operator in the NPAC for a served TN would normally be associated with that TN's geographical area (e.g., an east coast IP gateway is associated with an east coast TN) and stays static. The same may apply to the IP gateway info given to the IP-interconnection partners.

So the previous options may result in non-optimal routing in the IP domain for roaming mobiles as shown in Figure 1.

Please note that there may not be a transit operator between the originating operator and destination operator when they have peering points for direct interconnections.

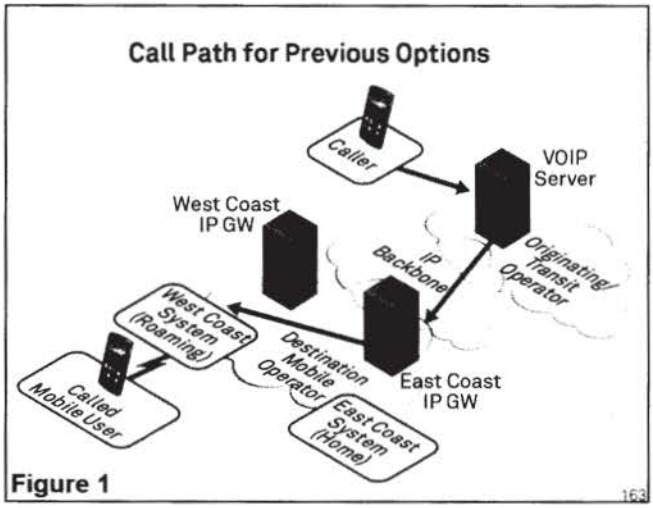


Figure 1

Praxis Solution

The proposed solution is to have the VOICE URI information for a mobile TN in the NPAC dynamically updated based on the mobile's roaming location. So when a mobile from the east coast system is roaming in a west coast system, the VOICE URI information provisioned in the NPAC would be changed from the east coast IP gateway to the west coast IP gateway. If a mobile operator provisions all the IP gateways in the NPAC with different preference values for alternate routing in case of IP gateway failure(s), the preference of the east coast IP gateway would be changed from the highest preference value to a lower value and the west coast IP gateway would be changed from a lower value to the highest value.

There are two options for a mobile operator to update the VOICE URI information in the NPAC.

1. The roamer's home mobile operator uses the existing NPAC Service Order Administration (SOA) interface or the Graphic User Interface (GUI) to update the VOICE URI information for the affected TN (e.g., change the VOICE URI strings or the preference values of the VOICE URI strings). This requires that the Home Location Register (HLR)/Home Subscriber Subsystem (HSS) or the IP Multimedia Subsystem (IMS) Call Session Control Functions (CSCFs) in the mobile operator networks notify its provisioning system when it detects the location change that requires updating the VOICE URI information in the NPAC.

2. The roamer's home mobile operator uses either an existing interface or a proprietary API to inform Neustar about the location of the mobiles. This avoids the effort for the mobile operators to enhance their systems to trigger their provisioning systems to use the NPAC SOA or GUI interface to update the NAPC.

   There are interfaces such as those used between the HSS and the Application Server (AS), between the CSCFs and the AS or between the HSS and the Gateway Mobile Location Center (GMLC) that can be used by Neustar to receive the mobile location information.

   The Neustar server that supports such interface(s) to some of the mobile operators would need to obtain beforehand the area covered by each of the IP gateway from each of the mobile operators using such interfaces. When the Neustar server receive the location information from a mobile operator for a TN, it can determine the appropriate IP gateway for that location and use the NPAC GUI interface to update the VOICE URI information for the affected TN in the NPAC when needed.

After the VOICE URI information is updated in the NPAC, the NPAC broadcasts the update via the Local Service Management System (LSMS) interface as is done today. The network operators and VoIP service providers then use the updated VOICE URI information for routing to the affected TN.

Figure 2 shows that the routing of an incoming VoIP call to a roaming mobile is optimized with this solution when an east coast mobile roams to a west coast system.

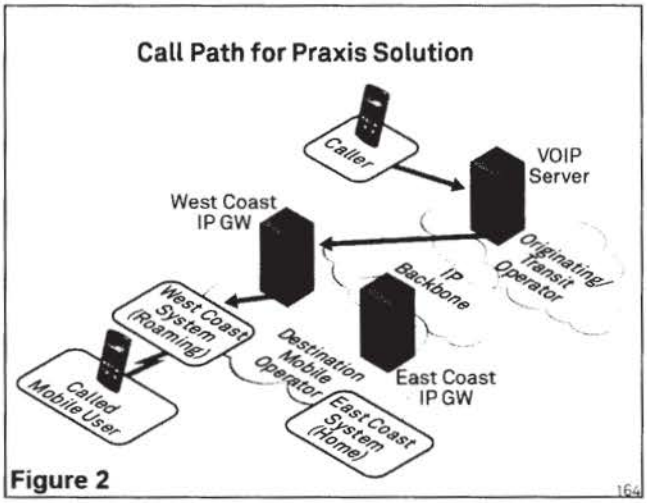


Figure 2

The saving is obvious for the destination mobile operator. The IP packets for the incoming VoIP call is now transported between the west coast IP gateway, which is much closer to the roaming mobile, and the west coast system.

For the originating/transit operator, the saving is realized when its IP gateway that handles the outbound VoIP call is located in the west coast. However, there is no saving for the originating/transit operator if its IP gateway is located in the east coast. In this case, the IP gateway can choose not to use the VOICE URI information from the NPAC if it is provisioned with the destination operator's east coast IP gateway information and sees that the IP gateway from the NPAC is not a good choice from its perspective.

The interconnection-agreements between the originating or transit operator and the destination mobile operator would impact how the incoming VoIP calls to the destination mobile operator are handled and routed by the originating or transit operator.

Benefits

- The destination mobile operator is benefited when the IP gateway that is close to the roaming mobile is the one to receive the incoming call. A roaming mobile would normally stay in the roaming mobile system for a while so the frequency of updating the VOICE URI information in the NPAC is not often.
- The originating or transit operator is benefited when its IP gateway that handles the outbound VoIP call is close to the IP gateway specified by the VOICE URI information received from the NPAC.
- The mobile operators can use the existing NPAC SOA or GUI interface to update the VOICE URI information in the NPAC for the affected TNs. The operators, mobile or non-mobile, and the service providers can receive the dynamically updated VOICE URI information over the existing LSMS interface.
- It avoids enhancement to the mobile operators' system to support this solution if they treat Neustar server as an AS to receive the mobiles' location information. Neustar may be able to charge for the service.
- The delays in media exchanged between the calling and called devices are slightly reduced because the IP packets travel less distance between the devices and possibly less routers. The reduction may look small in msec. (e.g., 10 msec.) but is actually not small when comparing with the actual time that an IP packet is transported from one device to another. The voice quality could be slightly improved.

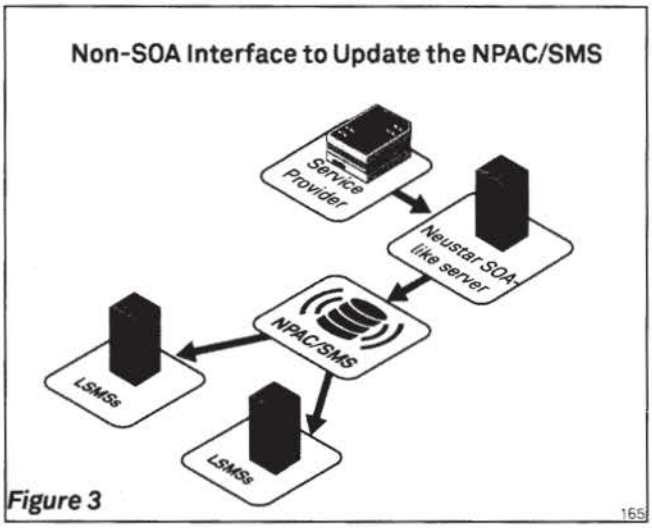
Implementation

The mobile operators can use the existing NPAC SOA or GUI interface to update the VOICE URI information for their affected TNs. The mobile operators would need to enhance their systems to support this solution. There is no impact on the NPAC except for more requests over the SOA or GUI interface and more broadcasts over the LSMS interface.

If the mobile operators uses the interface to an AS or a proprietary interface specified by either a mobile operator or Neustar to inform Neustar about the mobiles' location information, Neustar would need to deploy a server to receive the mobiles' location information and also obtain the serving area

for each of the IP gateway from the requesting mobile operators beforehand so as to be able to determine the IP gateway based on a mobile's location and update the VOICE URI information in the NPAC via the NPAC GUI interface for the affected TN when needed.

Figure 3 shows the high-level interactions among the involved systems/entities when a non-SOA/ non-GUI interface is used.



Conclusion

This white paper describes a solution that makes use of the NPAC to update the VOICE URI information for an affected TN when its associated mobile roams to a mobile system that can be accessed via an IP gateway that is closer to the mobile system where the mobile is roaming.

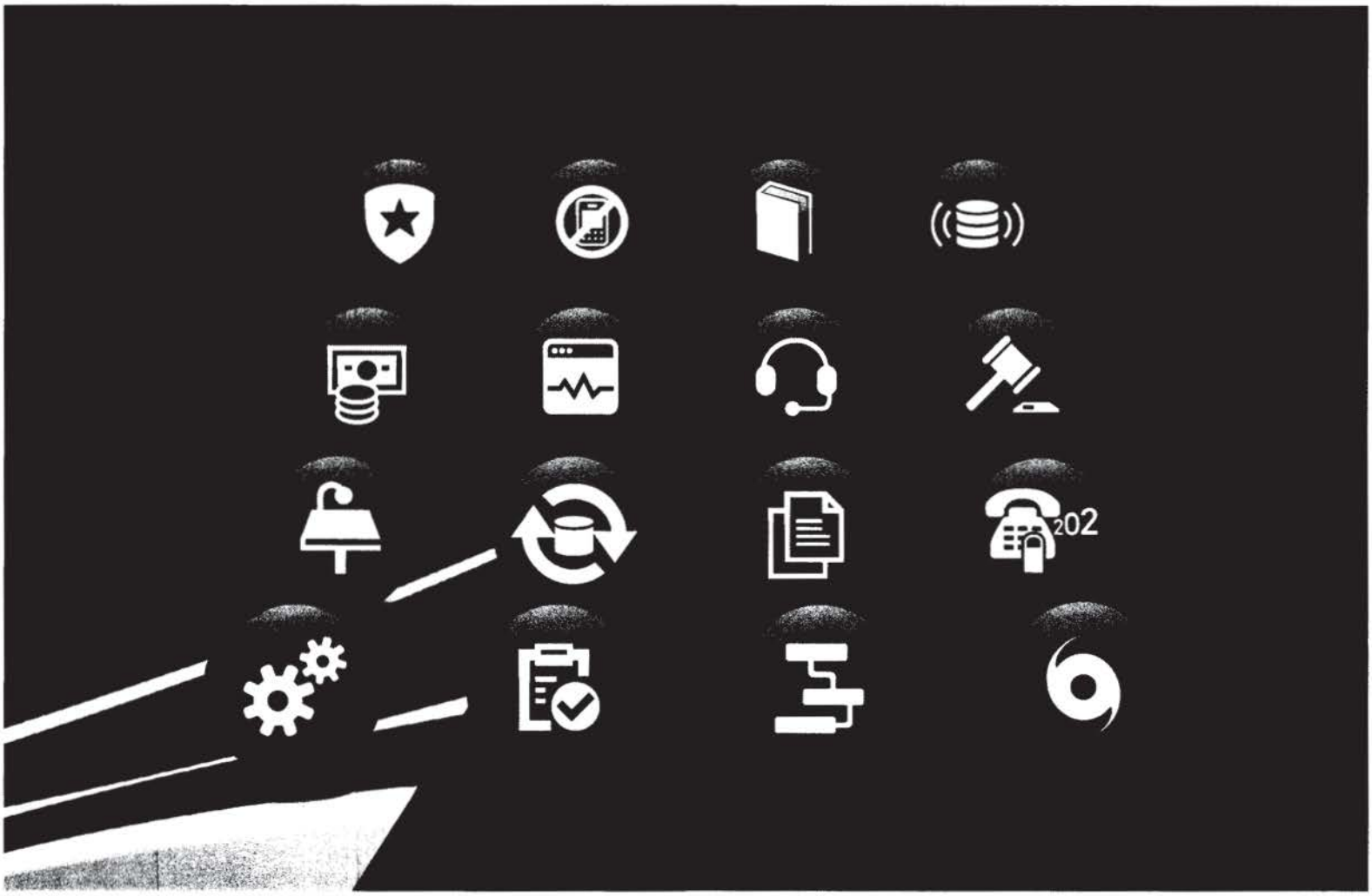
The mobile operators can use the existing SOA or GUI interface to update the VOICE URI information in the NPAC as is done today. Some can use a non-SOA or non-GUI interface to inform Neustar about the mobiles' location information so that Neustar updates the VOICE URI information in the NPAC on behalf of the mobile operators when needed.

The VoIP call path, when optimized, would benefit the destination mobile operator and it may benefit the originating/transit operator in certain routing scenarios. The media exchanged between the calling and called devices could travel a shorter distance that could result in a better voice quality.

Abbreviations Used in This Document

Acronym	Definition
[illegible]	[illegible]
CSCF	Call Session Control Functions
[illegible]	[illegible]
HSS	Home Subscriber Subsystem
[illegible]	[illegible]
GMLC	Gateway Mobile Location Center
[illegible]	[illegible]
IMS	IP Multimedia Subsystem
[illegible]	[illegible]
NPAC	Number Portability Administration Center
[illegible]	[illegible]
SIP	Session Initiation Protocol
[illegible]	[illegible]
URI	Universal Resource Identifier
[illegible]	[illegible]
SMS	Short Messaging Service
[illegible]	[illegible]
TN	Telephone Number
[illegible]	[illegible]
VoIP	Voice over Internet Protocol

Data Format Recommendations for Voice/SMS/MMS URI Fields in the NPAC



neustar®
Real **Intelligence.** Better **Decisions.**

Introduction and Overview

This whitepaper proposes data format recommendations for three of the five recently added Uniform Resource Identifier (URI) fields in the NPAC across all U.S. and Canada regions. Currently, the NPAC database contains the following URI fields for 7-digit number pool blocks and 10-digit Telephone Numbers (TNs):

1. VOICEURI
2. SMSURI
3. MMSURI
4. PRESURI (currently, only available for use in Canadian region)
5. POCURI (currently, only available for use in Canadian region)

Each of these URI fields can contain an ASCII string of up to 255 characters, excluding the pipe character (|), or ASCII code 0x7C (See NPAC Functional Requirement RR3-3: NPAC Service Management System Input Restrictions). Data format recommendations for the VOICEURI (NANC 429), SMSURI (NANC 435) and MMSURI (NANC 430) are proposed in this whitepaper and look to leverage existing industry standards, where available and applicable. Where industry standards are not available, modest extensions to established ones are suggested. Industry feedback on these proposed recommendations is encouraged.

Use of the NPAC for IP Service Communities

The NPAC URI fields can be used for:

1. Broadcasting text messaging capabilities on wireline numbers (whitelisting). If special commercial arrangements are not made for this today, SMS and/or MMS delivery to non-wireless telephone numbers will fail.
2. Broadcasting IP-based voice termination points, similar to Destination Point Codes (DPCs), of where to discover specific IP-based voice termination routing information. This use case has been gaining momentum in light of recent regulatory positions and proposed rule makings.

Using an established, authoritative, and neutrally administered registry for these use cases can help save costs relative to existing ad hoc and manual approaches, as well as improve data quality and integrity since now the relevant information is consolidated into one, industry-recognized, authoritative database. (Note: in 2010, as a means of mitigating the capacity constraints of traditional LSMSs, the NPAC was modified per NANC change order 442 to allow for telephone numbers to be provisioned with all 0's in the LRN field. These NPAC records, known as "Pseudo-LRN" records, are designed to store a broader set of telephone numbers and associated attributes, such as NPAC URIs.)

High-level Solution

Although the population of NPAC URI fields is increasing, it is generally held that a set of industry guidelines are required so that all participants in the various ecosystems can efficiently automate direct use of these optional fields in a common way. NPAC URI field values populated today are fully qualified domain names or host names and do not comply with standard URI syntax, as specified in IETF RFC 3896.

Since URI fields are generally intended for IP-related services, DNS ENUM specific URI schemes should be followed, as specified in IETF RFC 6118. If the NPAC URI fields are not used, additional routing mechanisms will be required. The proposed use of these NPAC URI fields is consistent with the concept of DPCs, as well as with more commonly referenced carrier ENUM (tiered) architectures.

Neustar's Data Format Recommendations

The following sections contain three important recommendations:

1. Recommendations for the SMSURI, MMSURI and VOICEURI data fields
2. Recommendations for supporting multiple URI values within a single field
3. Recommendations for Tier-2 delegations as further defined below

SMSURI Format

RFC 6118 contains the following two scheme definitions, as specified by IETF RFC 4355:

- sms:mailto
- sms:tel

The recommended value for the SMSURI field in NPAC is one of the following URI schemes:

- mailto:
- tel:

The mailto: URI syntax is specified by IETF RFC 6068. The following is an example:

mailto:\1@sms.example.com?spid=X109

which would be mapped into a NAPTR record, such as:

IN NAPTR 10 10 "u" "E2U+sms:mailto" "!^(.*)$!mailto:\1@sms.example.com?spid=X109!" .

The tel: URI syntax is specified by IETF RFC 5341. New parameters, such as "spid", are needed to carry additional data fields, such as:

tel:\1;rn=7035551234;npdi;spid=X109

which would be mapped into a NAPTR record, such as:

IN NAPTR 10 10 "u" "E2U+sms:tel" "!^(.*)$!tel:\1;rn=7035551234;npdi;spid=X109!"

Note: IETF RFC 4694 defines Number Portability (NP) related parameters, while IETF RFC 4904 specifies parameters related to trunk groups. The "spid" parameter is recommended to be defined by NPAC Functional Requirement RR4-6: New Service Provider ID and CMIP ASN.1 Data Type Definition:

GraphicFixedString4 ::= GraphicStringBase(SIZE(4))

ServiceProvId ::= GraphicFixedString4 -- (must be 4 alphanumeric characters).

New tel: URI parameters, such as "spid", would be registered with IANA at:

http://www.iana.org/assignments/tel-uri-parameters/tel-uri-parameters.txt

and would follow IETF recommendations for avoiding any possible conflicts.

MMSURI Format

RFC 6118 contains the following two scheme definitions, as specified by RFC 4355:

- mms:mailto
- mms:tel

MMSURI values are recommended to follow the same formats of the SMSURI values, except that the URI scheme is mms, instead of sms.

VOICEURI Format

RFC 6118 contains the following five scheme definitions for voice-related DNS ENUM services:

- pstn:tel IETF RFC 4769
- pstn:sip IETF RFC 4769
- h323 IETF RFC 3508
- sip or sips IETF RFC 3764
- voice:tel IETF RFC 4415

Because RFC 3764 is an older version of the more generic SIP related protocols, RFC 4415 is more related to peer-to-peer interactive voice sessions, and "h323" would be required for supporting some existing regulated services (e.g., Telecommunications Relay Service), the proposed recommendation is to support the following three URI schemes:

- pstn:tel
- pstn:sip
- h323

with the corresponding DNS ENUM service names, such as:

- e2u+pstn:tel
- e2u+pstn:sip
- e2u+h323

The following are example URI values for each of the above schemes:

- tel:\1;rn=7035551234;npdi;spid=X109
- sip:\1;rn=7035551234;npdi@example.com;user=phone
- h323:\1@example.com

These would in turn be mapped into NAPTR records, such as:

- IN NAPTR 10 10 "u" "E2U+pstn:tel" "!^(.*)$!tel:\1;rn=7035551234;npdi;spid=X109!"
- IN NAPTR 10 10 "u" "E2U+pstn:sip" "!^(.*)$!:\1;rn=7035551234;npdi@example.com;user=phone!" .
- IN NAPTR 10 10 "u" "E2U+h323" "!^(.*)$! h323:\1@example.com!" .

Again, any new tel: URI parameters, such as "spid", would be registered with IANA.

Multiple URI Values

It may be desirable to provision multiple URI values into a single NPAC URI field, e.g., to represent different URI values, redundant name servers, etc. To facilitate this, a URI value separator or delimiter is required. If the character used as the separator or delimiter occurs in a URI value, it should be encoded as %XX, where XX is the hex value of the character. This chosen character is proposed to be an ASN.1 GraphicString character other than "|" (0x7C), which is currently reserved by NPAC.

The order of multiple URI values in a single URI field may be used to derive the order or preference values of NAPTR records. For example, if "!" (hex 0x21) is chosen as the separator, a VOICEURI field with both sip and tel URI values can be specified as:

sip:\1;rn=7035551234;npdi@example.com;user=phone!tel:\1;rn=7035551234;npdi

which would be mapped into two NAPTR records, such as:

IN NAPTR 10 10 "u" "E2U+pstn:sip" "!^(.*)$!:\1;rn=7035551234;npdi@example.com;user=phone!" .

IN NAPTR 10 20 "u" "E2U+pstn:tel" "!^(.*)$!tel:\1;rn=7035551234;npdi!" .

with the sip URI value as the preferred one.

Please note that the LNPA Working Group may need to decide what can be populated in the URI fields, such as:

- rn
- spid
- svtype
- altspid
- lastaltspid
- other?

with a mandatory set, such as "rn" and "spid", and an optional set, such as "svtype" or "altspid", etc. Neustar is open to making such recommendations via its representatives to the LNPA Working Group.

Tier-2 Delegation

A Tier-2 delegation in NPAC would be comparable to standard DNS delegation where an authoritative name server for an IP domain receives a request for a sub-domain's records and responds with records for the other name servers.

Two possible mechanisms could be used to facilitate Tier-2 delegations in the NPAC database:

1. Populating non-terminal NAPTR records.
2. Directly specifying name server records.

Non-terminal NAPTR Records

If the URI value populated is simply a fully qualified domain name, it would be treated as a non-terminal NAPTR record, defined by IETF RFC 2915 and IETF RFC 6116.

For example, if the VOICEURI field is:

carrier-a.example.com

The corresponding NAPTR record would be:

IN NAPTR 10 10 "" "e2u" "" carrier-a.example.com

For example, after receiving the non-terminal NAPTR record, an ENUM client would perform a

DNS name server lookup for zone:

carrier-a.example.com

and then send the lookup query to one of the name servers returned, after replacing the terminating domain name to "carrier-a.example.com" in the query string.

Name Server Records

If the URI value populated starts with a scheme, such as "ns:" (TBD), it would be treated as a name server record, defined by IETF RFC 1035.

For example, if the VOICEURI field is:

ns:ns1.example.com!ns:ns2.example.com

The corresponding name server records would be:

IN NS ns1.example.com

IN NS ns2.example.com

Name Server Records:

- Pros: Uses well documented name server mechanism without extra lookups
- Cons: A new schemes needs to be defined for specifying name servers

Benefits to Industry

This whitepaper has proposed data format recommendations for URI fields in the NPAC. Using an established, authoritative, and neutrally administered registry for IP Service Communities can help save costs relative to existing ad hoc and manual approaches, as well as improve data quality and integrity since now the relevant information is consolidated into one, industry-recognized database. The adoption of existing industry standards for this relevant information further encourages broad adoption and high levels of integration across NPAC service order administration and local service management systems, as well as the addressing and routing platforms used by Service Providers.

Reference Material

So that all readers may follow the presentation and recommendations made in this whitepaper, we provide two important sources of reference that went into the research and writing of the document:

- Descriptions of the Internet Engineering Task Force Request for Comment (IETF RFC) standards used in this document
- Definitions of abbreviations used in this document

IETF RFC Standards Used in This Document

The guidelines recommended in this whitepaper are primarily supported by the IETF RFC documents. The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The IETF RFCs referenced in this whitepaper and their latest publication dates are as follows:

- IETF RFC 1035 - Domain names - implementation and specification – 11/1987
- IETF RFC 2915 - The Naming Authority Pointer (NAPTR) DNS Resource Record – 09/2000
- IETF RFC 3508 - H.323 Uniform Resource Locator (URL) Scheme Registration – 04/2003
- IETF RFC 3764 - ENUM service registration for Session Initiation Protocol (SIP) Addresses-of-Record – 04/2004
- IETF RFC 4415 - IANA Registration for ENUM service Voice – 02/2006
- IETF RFC 4694 - Number Portability Parameters for the "tel" URI – 10/2006
- IETF RFC 4769 - IANA Registration for an ENUM service Containing Public Switched Telephone Network (PSTN) Signaling Information – 11/2006
- IETF RFC 4904 - Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs) – 06/2007
- IETF RFC 5341 - The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry – 09/2008
- IETF RFC 6068 - The 'mailto' URI Scheme – 10/2010
- IETF RFC 6116 - The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM) – 03/2011

Abbreviations Used in This Document

Acronym	Definition
DNS	Domain Name Server
ENUM	Electronic Numbering Mapping
IETF	Internet Engineering Task Force
LNP	Local Number Portability
NANC	North American Numbering Council
NP	Number Portability
RFC	Request for Comment
SMS	Short Messaging Service
TN	Telephone Number
VoIP	Voice over Internet Protocol

Telephony-Related Queries

neustar®
Real **Intelligence.** Better **Decisions.**

Introduction and Market Overview

Solution Highlights:

- ENUM adoption has been slow with its reliance upon DNS inhibiting maximum utility
- Growth in internet communication services and new entrants will drive additional use and needs from NPAC
- Telephone Related Queries, TeRQ, presents successor to ENUM with robust capabilities that enables custom queries
- TeRQ allows industry to grow into adjacent segments, services, and requirements that can be served by TNs

As telephone services increasingly migrate from the PSTN to the Internet, Internet applications require access to diverse information about telephone numbers. Voice-over-IP (VoIP) clients need to learn how to route calls based on telephone numbers. Web services want to deliver text messages to Internet-enabled smart phones.

Nearly fourteen years ago, ENUM was first issued as a standard for providing translations between telephone numbers and Uniform Resource Indicators (URIs) on the Internet. ENUM relied on the underlying infrastructure of the Domain Name System (DNS) for its query-response syntax and semantics. ENUM has frequently been positioned as a replacement for legacy PSTN database query protocols like TCAP. The intrinsic limitations of the DNS, however, have often been strained by the requirements for accessing information about telephone numbers. The DNS makes few provisions for authenticating the source of queries, however, so handling non-public information is constantly a challenge in ENUM deployments. The centralized and authoritative hierarchy of the DNS also proved a poor match for the actual procedures used to route telephone calls. For that reason, ENUM adoption has been slow outside of private deployments, and public ENUM federations, such as CC1 ENUM and the CableLabs Peer Connect registry, have had no practical impact for American consumers.

Over the last decade, however, the need for Internet applications to operate on telephone numbers has only grown more pressing. Today, many carriers across the globe have begun developing plans to migrate their entire PSTN infrastructure onto the Internet within the next decade. Further pressures come from emerging Internet communications providers, who unburdened with any legacy PSTN equipment and expenses, can more nimbly compete with services related to telephone numbers, and VoIP. As time goes on, more and more providers will want to access the NPAC via the Internet, and the fields of the NPAC will undoubtedly change to reflect the changing requirements of deployments. The industry has a clear need for a next-generation standard for accessing information about telephone numbers over the Internet.

Neustar's Solution

Neustar therefore proposes a new protocol and interface for Telephony-Related Queries (TeRQ). As a successor to ENUM, TeRQ builds on existing Internet technology, but rather than focusing on the DNS layer, TeRQ runs at the application layer. This allows for richer queries and responses, increased security properties, and greater efficiency. As TeRQ does not couple its service to the hierarchical namespace servers of the DNS, it also allows far greater flexibility in deployment architectures as well.

TeRQ is a query/response protocol that enables a Client to send Queries to a Service about telephone numbers or related telephone services. Queries may pass through one or more Intermediaries on their way from a Client to a Service; for example, through aggregators or service bureaus. A client establishes the Subject of a Query, and optionally specifies one or more Attributes of particular interest in order to narrow the desired response. When a Service receives a Query, it performs any necessary authorization and policy decisions based on the Source. If policy permits, the Service generates a Response, which will consist of a Response Code and one or more Records associated with the

Subject. The Service then sends the Response through the same path that the Query followed; transactional identifiers set by the Client and Service correlate the Query to the Response and assist any intermediary routing.

One of the unique strengths of this architecture is the distributed authority model it offers. Authorities provision Records into Services (via protocols such as DRINKS), and thus is it possible for Records to contain a signature from Authorities that can be verified by either Intermediaries or Clients. This allows for the preservation of end-to-end security when intermediaries are present, and even enables multiple Authorities to provision records associated with the same telephone number. As new services associated with telephony become available, this flexibility will be critical to maintaining competitive services that are compelling to end users. This authority-driven approach will also be critical to authorizing communications, and thus for functions like spam prevention and fraud management.

Since the world of applications that interact with telephone numbers is growing more diverse, TeRQ must be capable of operating in different application environments. For that reason, TeRQ is defined as a protocol that will be carried over an existing standard, such as HTTP for the web world or DIAMETER for emerging mobile telephone networks. This independence of underlying transport also makes TeRQ future-proof, as new encodings and bindings can be developed to support new standards as they emerge.

Today, Neustar is working towards standardizing TeRQ at the Internet Engineering Task Force (IETF). More information about the nature of the protocol and the status of work can be found on the IETF's web site. As we consider the longer term implications for the NPAC, two requirements can be considered:

- The NPAC should add an attribute to each SV and pooled block to designate the location of a Service Provider's TeRQ host server on its IP network. This field would behave in much the same way as the NPAC's existing SS7 DPC's, including CNAM – to inform other Service Providers where on the network they should look to retrieve information about the TN using the TeRQ protocol.
- The NPAC should be enabled to interact with Service Providers using the TeRQ protocol. For example, as a long-term replacement to the Inter-Carrier Process (ICP), TeRQ queries to the NPAC can be used to perform subscriber validation prior to the porting process.

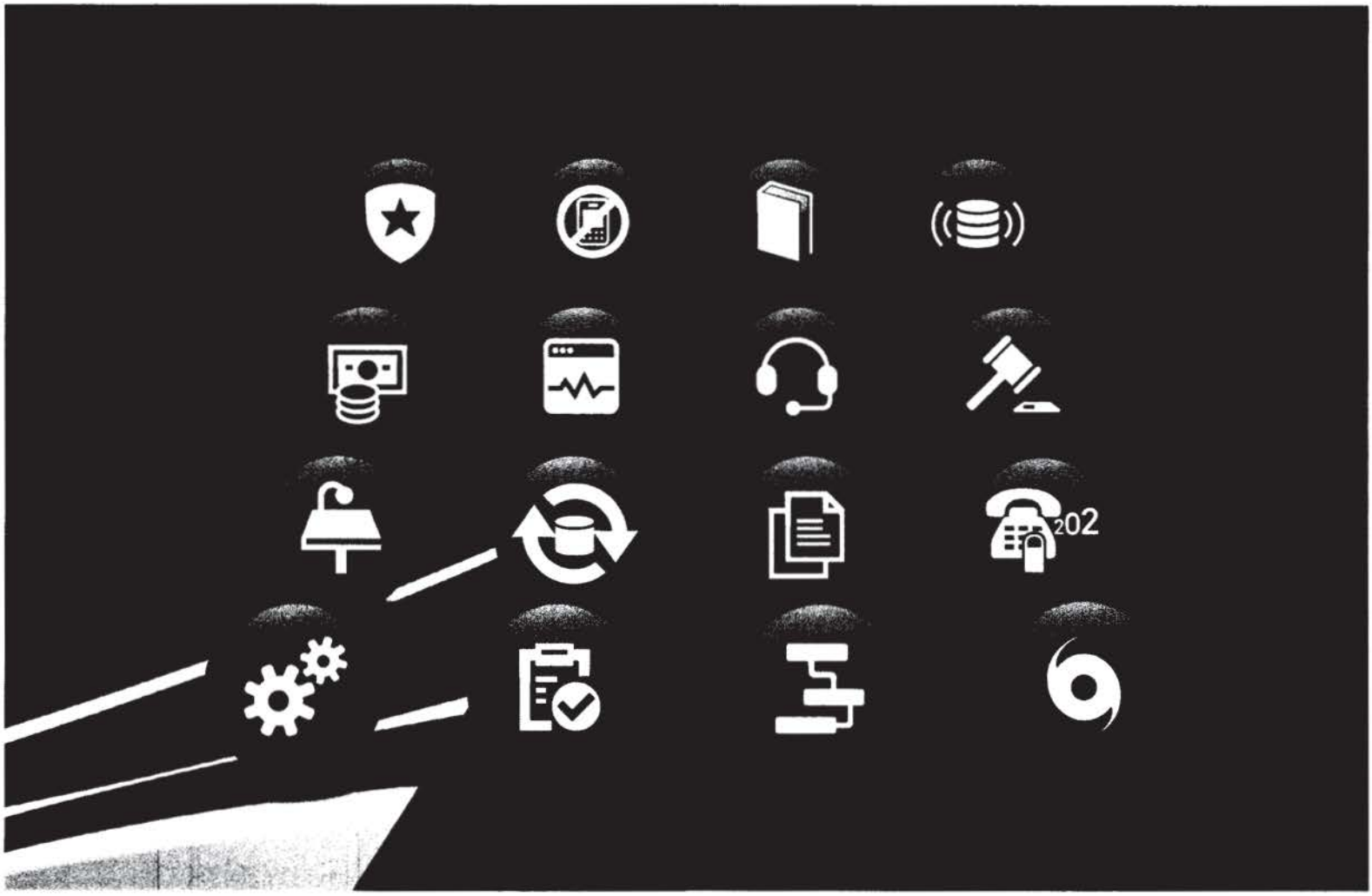
Benefits to the Industry

TeRQ makes it possible for the NPAC community to grow beyond the confines of the PSTN, and to incorporate the new services and requirements that telephone numbers will encompass. With TeRQ, it will be simpler for existing PSTN Service Providers to migrate their networks onto the Internet, as well as for new Internet-based providers to gain access to critical information necessary to use telephone numbers to their fullest. The inherent distributed architecture of TeRQ does not require the top-down hierarchical model that constrained ENUM, and thus is faces far fewer hurdles to deployment. Moreover, the solution has a much stronger security story than ENUM, which again makes TeRQ more likely to succeed in an open Internet environment.

Abbreviations Used in This Document

Acronym	Definition
CNAM	Caller ID Name
DPC	Data Point Code
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
NPAC	Number Portability Administration Center
SS7	Signaling System 7
TCAP	Transaction Capabilities Application Part
TN	Telephone Number
VOIP	Voice Over Internet Protocol

Telephone Numbers as Secure Universal Identifiers



neustar®
Real **Intelligence.** Better **Decisions.**

Introduction and Market Overview

Telephone Numbers (TNs) have long been used as an identity by individuals and businesses, extending far beyond communications Service Providers. As everything moves to the Internet, TNs continue to be used as an identity, but their usefulness becomes limited as validation techniques grow more cumbersome. Associating digital certificates to TNs through the authoritative registry provided by the NPAC will greatly enhance the ability to leverage TNs as validation for subscriber identity.

Solution Highlights:

- Growth of Internet based calls increase need to provide secure identities and reduce malignant abuses such as spoofing
- Assigning digital credentials to TNs presents a solution for secure and reliable identity management
- NPAC's certificate authority capability can be extended to support robust and secure authentication of TN over IP
- Evolution of Internet and networks creates opportunities to extend value of TN through digital certificates, specifically with:
  - Digital certificates as primary identifiers
  - Digital identity registers
  - Personal clouds

Since TNs are globally unique, easy to store and transmit, and likely to persist with a particular individual (thanks to portability), many businesses will rely on them to uniquely identify a customer. Some even going so far as to use a telephone number as an account name. TNs serve well for this purpose because they are easily associated with names, addresses, and billing relationships with carriers. Given the many security concerns that confront the provisioning and delivery of Internet services, the reliability of TNs as stable customer identifiers offers a number of advantages over other Internet identifiers like email addresses. For example, it is now common practice for financial web sites to text a phone number to verify an individual who is attempting an unusual transaction, as this provides a secure "out of band" form of dual-factor authentication.

As telecom networks evolve toward Internet Protocol (IP) technology, a clear need arises to bind cryptographic credentials to TNs as reliable identifiers for individuals and to prevent unauthorized spoofing. Today, a blatant security gap exists as there is no secure way to validate the recipient of a call or message to a particular TN. Similarly, a potential problem also arises when identifying the source of telephone calls over the Internet. Caller ID is no longer a 100% reliable indicator; there are even telemarketing companies that launch calls from the Internet, claiming a fake Caller-ID, through gateways to the PSTN to spoof their originating telephone numbers. They do this to increase the chance that targets will answer the phone.

Assigning and administering digital credentials to subscribers can be a mechanism for Service Providers to drive additional value and build upon the affinity their customers have for their numbers. As the assignee of TNs to end users, communications Service Providers are in a unique position to take advantage of this widely used and understood form of identity. Extending the functionality of TNs in this manner can enable them to become the primary secure identity for cyberspace.

Neustar's Solution Concept

In order for TNs to serve as reliable identifiers on the Internet, they must be associated with a digital credential that can then be shared in IP communications, assuring that an entity on the Internet can legitimately claim authority for a number. Once the identifier is secured, it could be used for many applications that depend upon secure and reliable identity management, such as mobile finance and health care-related services.

Such a credential, once assigned, could be used to battle spoofing by providing a means to

authenticate the originator of phone calls and text messages over the IP network. RFC 4744, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol," edited by Jon Peterson (a Neustar Fellow), defines a mechanism using digital certificates for securely identifying originators of SIP messages. This mechanism is designed to work with the sorts of digital certificates in use on the web today; that is, certificates that cover an Internet domain name. However, while extensive public key infrastructures already exist for the web, there is no similar certificate authority for telephone numbers. So, applying RFC 4474 to telephone numbers requires an authoritative root of trust for a new category of telephone number-based certificates.

For the North American Numbering Plan, the NPAC is a natural location for this certificate authority to reside. This capability will first and foremost allow for more secure TN routing and Caller-ID on the Internet (both for calls and text messages) – a natural extension of the NPAC's current role.

It happens that the need for such a credential has already arisen organically in NPAC operations. The NPAC has recently implemented a certificate authority (CA) for enabling secure access by Service Providers to perform porting and network management functions on their inventories (this replaces the previously-used Secure ID tokens distributed to carriers). With only minor modifications, this same authentication mechanism can be extended, first to assign to a certificate a specific scope of authority over one or more TNs, verifiable by other Service Providers with access to the NPAC. With additional new messaging interfaces that validate certificates and telephone number ownership, the NPAC as a part of its standard call-routing functions could then offer a security step for terminating Service Providers seeking authoritative validation Caller-ID.

To illustrate, a VoIP provider could place a SIP call from a particular TN and include in it (via RFC4474 Identity-Info header field value or a similar mechanism) a reference to a certificate with authority over the TN in the From header field value. Recipients of the call could use a variety of standard protocols, including the Online Certificate Status Protocol (OCSP), to verify the authority of the certificate over the calling TN via the NPAC. Such a solution will verify that the call came from the Service Provider that was assigned the TN.

Because the NPAC is a neutrally-administered authoritative registry, and the entities that provision it are the Service Providers of record for the assigned TNs, the data can be trusted: the NPAC is the natural place to anchor a public key infrastructure for TNs.

Adding certificate holder attributes can expand this baseline solution to serve further needs of the NPAC community. For example, carriers increasingly want the ability to delegate certain NPAC provisioning capabilities to external parties such as resellers. With the approval of the primary, network-facing Service Provider, a reseller could be issued digital certificates that allow them to provision changes to limited fields in the NPAC (e.g. the URIs) for a specific range of delegated TNs, assigned to them by the primary. When the reseller establishes a connection with the NPAC and presents its certificate, the NPAC verifies the capabilities of that user with the certificate. This can streamline operations and optimize inventory management across the two companies.

One can extend the use cases even further. Digital certificates could be issued even to end users, as a means to enable third party authentication. Today, many websites and online applications use a subscriber's TN to identify them. This can be done by sending a text message to the user and taking them through a validation step (e.g., click a personalized link or enter a PIN code). To greatly streamline the set up process, the user could submit a certificate along with other credentials with the website verifying the TN with the NPAC.

These are just a few examples of how linking a certificate to a TN through the NPAC could confer the intrinsic security of TN to identity online.

Beyond TNs and Number Portability

The implementation of local number portability serendipitously protected the value of the phone number. With portability and the ability to permanently retain one's telephone number came a resilient and enduring identifier, one that continues to be used in many spheres beyond making phone calls (for example, loyalty cards). If portability had not been required, it is reasonable to ask whether telephone numbers would still have such an affinity, or whether another personal identifier would have taken ascendancy. Or, would consumers have a more fragmented identifier landscape than today? In either case, the Service Provider business landscape would have been altered significantly.

The NPAC provides the foundation for the continued utility of the phone number as an identifier, which is critical given the ongoing demand for telephone numbers by the general public. However, as networks, devices and the Internet evolve, Service Providers should continue to explore whether the phone number is the only identifier that Service Providers might use for persons or things on their networks.

We suggested earlier in this paper that a TN could be associated with a digital certificate for IP communications thus providing further security for its use as an identifier. This extension of the NPAC continues to put primacy on the telephone number. As the industry considers the evolution of the NPAC through 2020, the following additional (not necessarily dependent) evolutions should be evaluated:

1. Adding additional identifiers in the NPAC, beyond just TNs. TNs and other identifiers would be associated with the digital certificate.
2. Extension of the NPAC to a digital identity registry for use by consumers, offered by their Service Providers.
3. Allowing subscribers to link the digital identities (administered by their Service Providers) to online meta-services such as Personal Clouds.

Digital Identities

As networks evolve, it may be desirable to enable routing, rating, and billing via additional identifiers beyond phone numbers. Or, it may be desirable to link various identifiers together as a Digital Identity that is secured by a Digital Certificate.

In fact PKI and Certificate Authority (CA) technology are extremely mature, and the potential benefits of a centralized system are well understood, but no single vendor has ever been able to create a system with enough scale and ubiquity to be truly useful. The NPAC is arguably the only system in place today that could serve as the foundation for a successful and general purpose CA.

With a CA in place, linking and associating multiple device identifiers with single subscriber is straightforward. As we go beyond TNs to include additional identifiers, some examples of other device identifiers that could also be used on a network include:

- IP address
- MAC address
- FDA UDI
- Apple UDID

As devices become increasing abstracted or separated from the services people use (for example, virtual devices that run only in the cloud but remain users of the network), digital identifiers for the subscribers themselves can also be related to routing, rating and billing. Examples include:

- Email address
- OpenID
- XRI i-name or i-number
- Twitter handle

We could even get to the point where identifiers for content become necessary. For that, there are many interesting existing and emerging systems. Examples include:

- URIs
- Digital Object Identifiers
- UltraViolet

Enabling the NPAC to uniquely associate some of the above identifiers with subscribers would allow a highly flexible system for rating, routing and billing on the networks of the future.

Digital Identity Registry

The Internet is currently dominated by federated identity schemes that have achieved limited success because they could not establish both scale and durability to meet consumer expectations. As the NPAC expands to a universal TN registry, it will be in a position to maintain identifiers for almost every person in the US. It thus has the scale, authority, and durability required to dominate the digital identity landscape. Using the NPAC as the foundation for such a registry ensures that it would remain neutral, transparent, shared and under the auspices of the communications Industry.

Neustar has the technical know-how and experience to evolve the NPAC into an identity registry; based on digital certificates and/or identity registry technologies such as XDI, where Neustar has deep experience (Neustar operates the global XDI registry). XDI is both a discovery and registry service that enables persistent resolvable identifiers, as well as a semantic layer to enable well defined data interchange. This technology is foundational for Neustar's approach to personal clouds which is one of the applications of a digital identity registry

Personal Clouds

Consumers use multiple devices to access the same content and services. Cloud services such as Dropbox and iCloud and Google Apps further enable this general trend, moving storage and computing into the cloud. As consumers complete this shift and demand the ability, for example, to

access all of their personal data via the cloud or log in to all of their cloud services with a single or federated digital identity, the paradigm of "personal cloud" has started to emerge.

If we look beyond the narrow scenarios solved by each vendor mentioned above, a personal cloud ought to be a virtual wrapper around all of a consumer's cloud services and content – it's a meta-service. As such, digital identity is the cornerstone of a personal cloud, as that which links services and content together. But today there is no single identity service that is purpose-built for this use case (i.e., that would enable consumers to link their services and content together in meaningful ways), and thus the personal cloud space remains fragmented. What the web needs is a DNS scale service for real and permanent digital identity for personal clouds.

Neustar has been investing in this new type of identity service, using XDI (a global registry, discovery service, and data exchange protocol) to link data, devices and resources to a single identity, thus creating a "personal cloud." We're also developing an open source fabric that will enable an ecosystem of apps and services for the new digital identities. We are developing prototypes with partners, we are founding members of the Respect Network and we are working within the OIX approved Respect Trust Framework. Neustar brings special qualifications to the table: we are the registry for XDI (as well as multiple TLDs such as .biz, .co, .tel, and 358 new TLDs), we have a strong legacy of trust and respect for personally identifiable information, and we are capable of deploying and managing internet scale services.

Figure 1 below shows what Neustar is intending to build in partnership with the Industry:

- Fabric and network services that will enable essential functions such as discovery (finding other clouds)
- XDI based personal data store, which will enable a semantic and policy layer for data, thus enabling clouds to link to each other and exchange data.
- Cloud OS for evented apps related to data

Proposed Architecture for the Personal Cloud Fabric Open Source Project

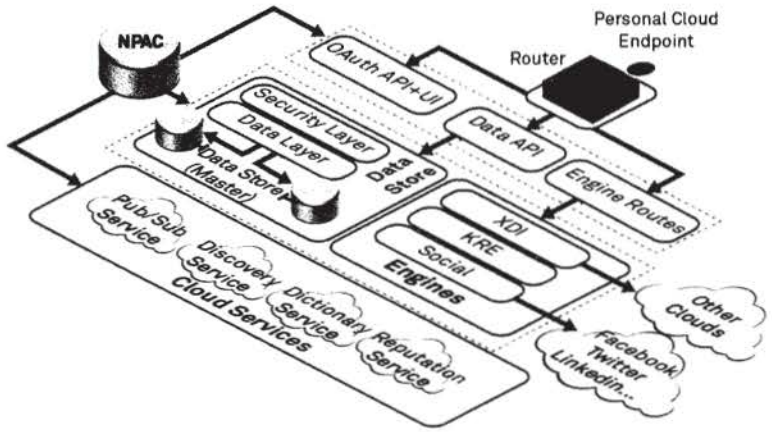


Figure 1

151

Just as the TN is the most important personal identifier in the world today, in part because of its portability that has created a sense of ownership and permanence in the minds of consumers, we believe the neutrality and scope of the NPAC is ideal for ensuring that the Service Providers, collectively, govern this emerging control point of the internet.

Abbreviations Used in This Document

Acronym	Definition
DNS	Domain Name System
MAC	Media Access Control
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
TLD	Top-Level Domain
URI	Universal Resource Identifier
UDID	Unique Device Identifier
XDI	XRI Data Interchange

Revenue by Segment

REDACTED--FOR PUBLIC INSPECTION

HIGHLY CONFIDENTIAL